FH OBERÖSTERREICH

Verunsicherte Kunden durch NFC

Wie sicher ist NFC wirklich?

Michael Roland

23. Oktober 2013 • IIR Payment Forum Cashless • Wien

NFC Research Lab Hagenberg

This work is part of the project "High Speed RFID" within the EU program "Regionale Wettbewerbsfähigkeit OÖ 2007–2013 (Regio 13)" funded by the European regional development fund (ERDF) and the Province of Upper Austria (Land Oberösterreich).

LAND OBERÖSTERREICH

NFC Research Lab Hagenberg • www.nfc-research.at
A research group of the University of Applied Sciences Upper Austria

Was ist eine Smartcard?

Lesegerät

Energie

Befehl

Antwort

Smartcard
(„Mini-Computer“)

Applikationen

Maestro

MasterCard

QUICK

VISA

V PAY

...

A1 T··

SIM-Karte

TRUST
einfach sicher

Bürgerkarte

Wie funktioniert eine Maestro-Transaktion?

Liste der verfügbaren Payment-Applikation anfordern

```
--> 00A404000E...
<-- 6F2C840F32...
--> 00A4040007...
<-- 6F298407A0...
```

Karte unterstützt Maestro

Maestro-Applikation auswählen

```
--> 80A800000A...
<-- 7716820219...
--> 00B2010C00
<-- 701A571367...
```

Applikationsparameter

Applikations-Konfiguration anfordern

```
--> 00B2020C00
<-- 70535F2403...
--> 00B2030C00...
<-- 701D9F4A01...
```

Konfigurationsparameter

Kartendaten (lt. Konfiguration) anfordern

```
--> 00B2011400
<-- 7081BC8F01...
--> 00B2021400...
<-- 709C9F4703...
```

Kartendaten

Transaktionsdaten an Karte senden und digitale Signatur anfordern

```
--> 00B2041400
<-- 7081C19F46...
--> 00B2012400...
<-- 702B8E0C00...
--> 80AE500042...
<-- 7781B29F27...
```

digitale Signatur über Transaktions- und Kartendaten

Im Detail: Welche Daten werden übertragen?

- Art und Parameter der Payment-Applikation
  - Maestro, …
- Kartendaten
- Transaktionsdaten (zur Signatur durch die Karte)
  - Betrag, Währung, Datum, Uhrzeit, Art, … der Transaktion
  - Länderkennung, Art, … des Terminals
  - Parameter des kryptographischen Signaturverfahrens
- Verifikationsdaten
  - Digitale Signatur über Transaktions- und Kartendaten

Im Detail: Welche Daten sind auf der Karte gespeichert?

- Maestro PayPass
  - PAN: Identifikationsnummer der Bank + Kontonummer
  - Gültigkeitsdaten
  - Land in dem Karte ausgestellt wurde
  - Währung in der die Karte abgerechnet wird
  - Liste der Daten zur Berücksichtigung bei der digitalen Signatur
  - Transaktionszähler
  - Protokoll über die letzten 10 Transaktionen *(in Zukunft nicht mehr)*
  - öffentlicher Schlüssel/Zertifikat des Kartenherausgebers
  - öffentlicher Schlüssel/Zertifikat der Karte
  - geheimer Schlüssel der Karte *(nicht auslesbar)*

Im Detail: Welche Daten sind auf der Karte gespeichert?

- Kreditkarte
  - wie bei Maestro
  - PAN: Kreditkartennummer
  - Name des Karteninhabers *(kontaktlos nicht auslesbar)*

Im Detail: Welche Daten sind auf der Karte gespeichert?

- Quick
  - Identifikationsnummer der Geldbörse
  - aktueller und maximaler Quick-Saldo
  - Währung
  - Gültigkeit (Aktivierungs-, Deaktivierungs- und Ablaufdatum)
  - Jugendschutzkennzeichnung
  - Protokoll der Ladevorgänge *(nicht bei NFC-Karten)*
  - Protokoll der Bezahlvorgänge *(nicht bei NFC-Karten)*

Bankomat-/Kreditkarte vs. Quick

vs.

Bankomat-/Kreditkarte

- Karte ist „nur“ Schlüssel zum Konto

Quick

- Karte enthält Geld

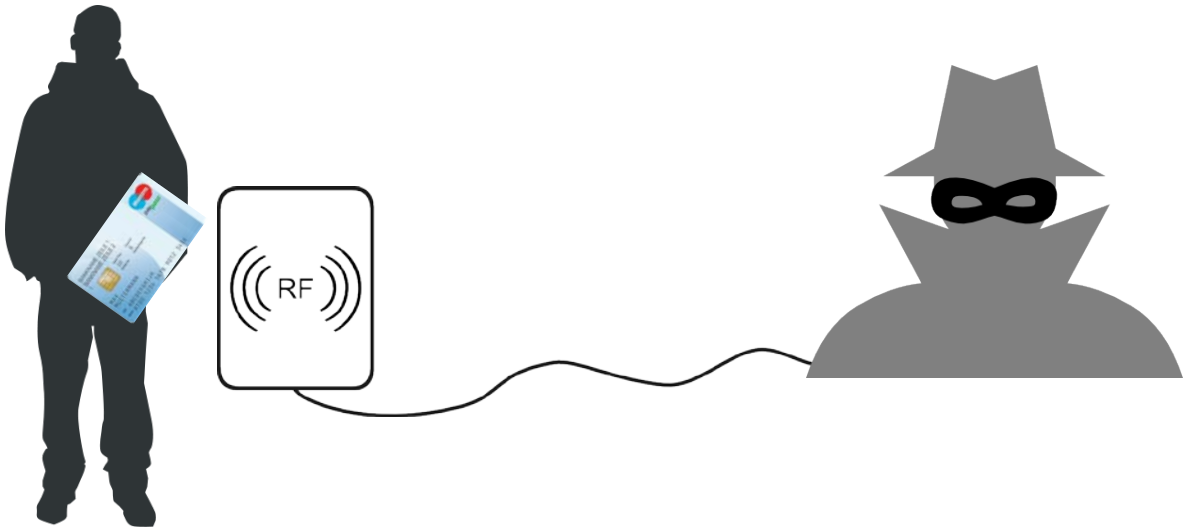
Bekannte Angriffsszenarien gegen NFC-Karten

- Eavesdropping
  - Mithören von Transaktionen
- Skimming
  - Auslesen von Daten
- Abbuchung im Vorbeigehen
  - Nutzung von Karten „im Vorbeigehen“ mit echtem Bezahlterminal
- Relay
  - Nutzung von Karten über große Entfernungen
- Preplay
  - Vorberechnen von Transaktionsdaten

Eavesdropping

- NFC = Funkübertragung
  - Kommunikation nur über wenige Zentimeter
  - ABER: Mithören auch über mehrere Meter hinweg möglich
- Angreifer: Informationen über Karte und aktuelle Transaktion ausspähbar
  - z.T. personenbezogene Daten (Kreditkarten-/Kontonummer, Quick-Guthaben, Betrag der aktuellen Transaktion)
  - Daten reichen **nicht** aus um weitere Kartentransaktionen durchzuführen oder Kartenkopie zu erstellen

Skimming



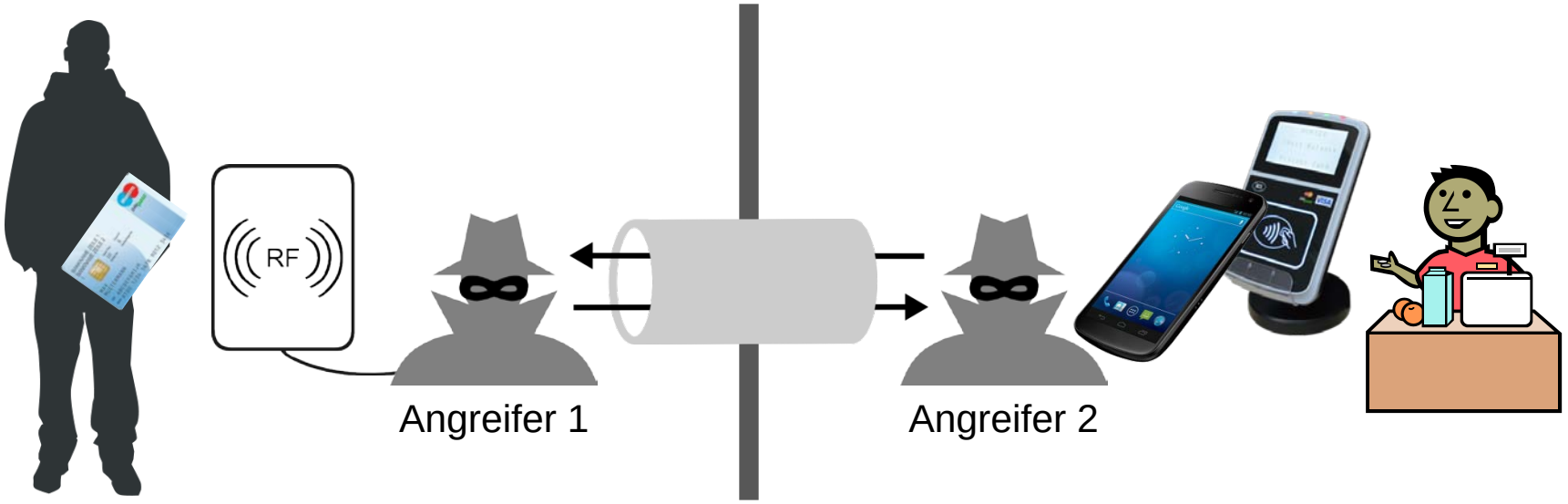
- Kartendaten frei auslesbar
  - z.T. personenbezogene Daten (Kreditkarten-/Kontonummer, Quick-Guthaben, ev. Protokoll der letzten Transaktionen)
  - **Nicht auslesbar:** geheime Schlüssel (notwendig für Transaktionen)
  - Daten reichen **nicht** aus um später Kartentransaktionen durchzuführen oder Kartenkopie zu erstellen

Abbuchung „im Vorbeigehen“

- Angreifer nutzt echtes Bezahlterminal um Geld abzubuchen
  - Nur möglich in Kombination mit Händlervertrag
  - Angreifer über Händlervertrag leicht identifizierbar

  → praktischer Nutzen für Angreifer sehr gering

Relay-Angriff



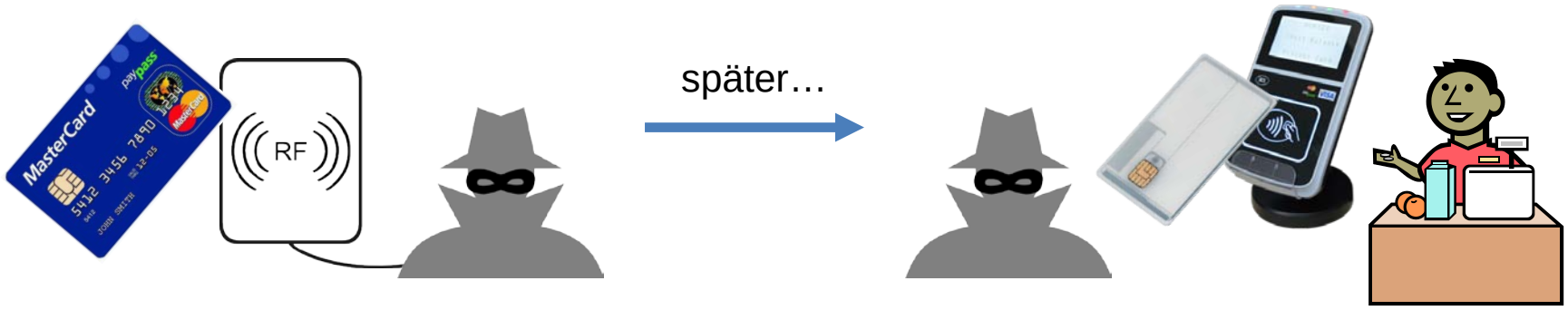
- Zwei Angreifer notwendig
  - Angreifer 1: bringt Lesegerät in Reichweite von Karte
  - Angreifer 2: bezahlt an Kasse
- Hürden für Angreifer
  - Angreifer 1 muss genau dann Kontakt zur Karte haben, wenn Angreifer 2 bezahlt
  - Zuverlässige Kommunikation mit Karte nur mit guter Positionierung des Lesegeräts möglich
  - Bankomatkarte in Österreich: Jede Transaktion ist auf € 25 beschränkt!
  - Es können nur Waren gekauft werden → praktischer Nutzen für Angreifer???

Video: Relay-Angriff

http://youtu.be/t0MCFjYHieQ

Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones (L. Francis et al.; RFIDsec Asia 2012)

Preplay-Angriff



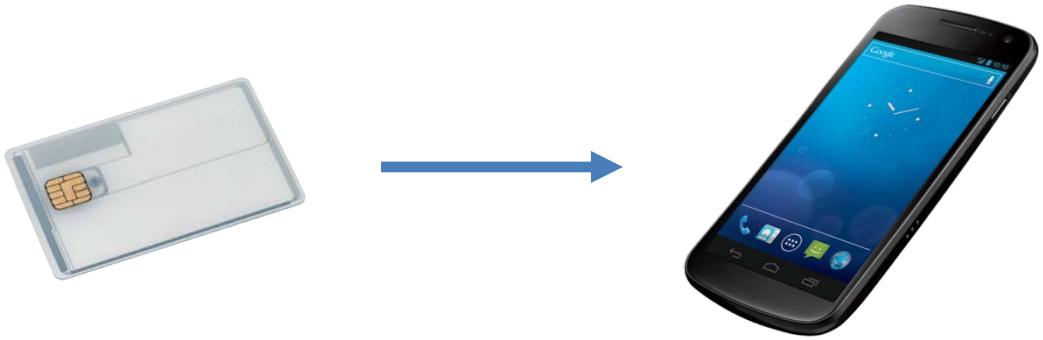
- Transaktionen
  - Angriff betrifft speziell MasterCard PayPass
  - ABER: Maestro PayPass (Bankomatkarte) **nicht** betroffen
- Skimming-Angriff mit Vorberechnung von Transaktionscodes
  - PayPass-Karten und -Terminals unterstützen neben sicherem EMV-Verfahren auch noch Mag-Stripe-Verfahren (für Rückwärtskompatibilität zu älteren Karten/Terminals)
  - Transaktionscodes für Mag-Stripe-Verfahren lassen sich mit Zugriff auf Kreditkarte in kurzer Zeit vorausberechnen
  - Mit Kartendaten und vorausberechneten Transaktionscodes lässt sich funktionsfähige Kartenkopie erstellen
  - Kartenkopie kann zum kontaktlosen Zahlen genutzt werden
- Schwachstelle durch Issuer einfach behebbar (PayPass sieht bereits Gegenmaßnahmen vor)

Video: Preplay-Angriff

http://youtu.be/VlAwxUs1ZFo

Cloning Credit Cards – A combined pre-play and downgrade attack on EMV Contactless (M. Roland, J. Langer; WOOT 2013)

Von der Karte zum Mobiltelefon…

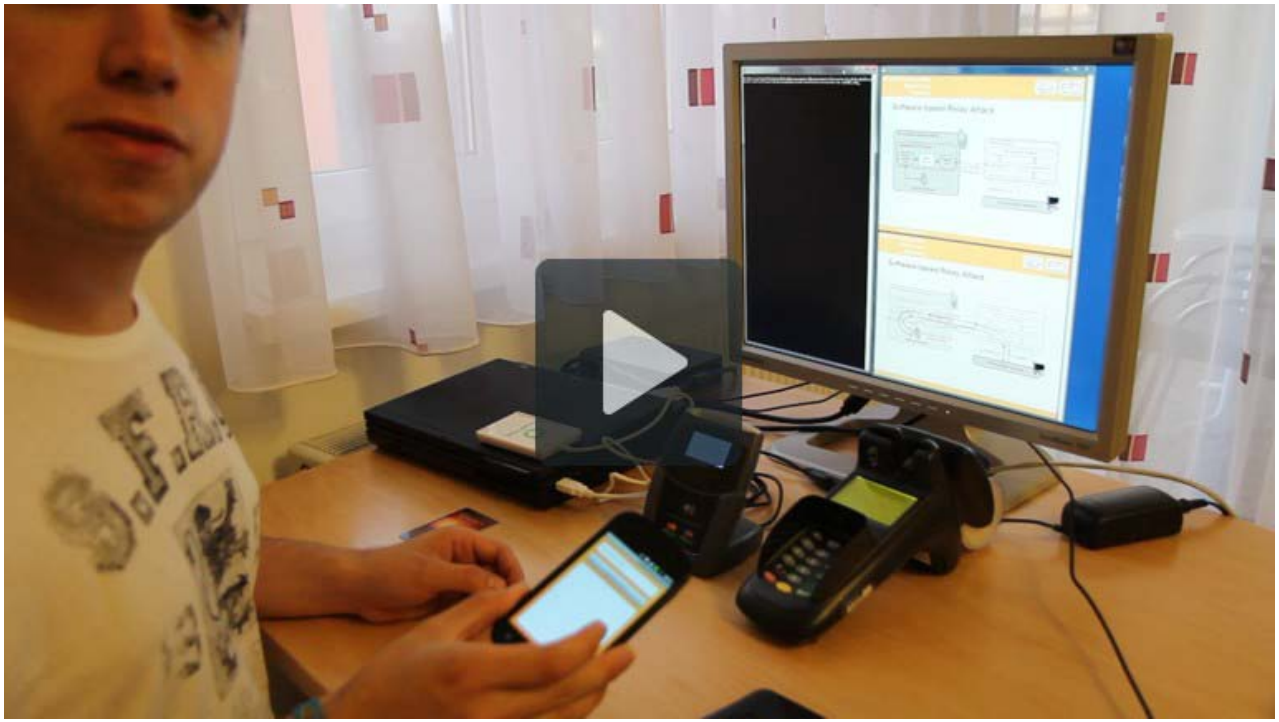


- Secure Element
  - sicherer Smartcard-Chip im Mobiltelefon
  - Applikationen für Karte passen auch auf Secure Element
  - Secure Element kommuniziert
    - mit Mobiltelefon-Apps über interne Schnittstelle
    - mit NFC-Lesegeräten über NFC-Antenne des Mobiltelefons

Sicherheit des Secure Element im Mobiltelefon

- Grundsätzlich vergleichbar mit Karte (gleicher Chip)
- Vorteile durch Mobiltelefon
  - Mobiltelefon als Benutzerschnittstelle zu Secure Element
    - Transaktionen am Bildschirm anzeigen
    - Liste der letzten Transaktionen
    - PIN-Eingabemöglichkeit
  - Secure Element für Mobiltelefon-Apps
    - kartenbasierte Zahlung im Mobiltelefon-Webbrowser / in Apps
- Nachteile durch Mobiltelefon
  - Apps haben Zugriff auf Secure Element
  - Mobiltelefon ist typischerweise **nicht** sicher
  - Apps können Secure Element Applikationen angreifen
    - Relay-Angriff (vgl. Google Wallet Relay Attack)
    - Schutzmaßnahmen möglich (schränken Einsatzmöglichkeiten des SE allerdings stark ein!)

Video:
Google Wallet Relay Attack



http://youtu.be/_R2JVPJzufg

Applying Relay Attacks to Google Wallet (M. Roland et al.; NFC 2013)

Dr. Michael Roland

Research Associate, NFC Research Lab Hagenberg
University of Applied Sciences Upper Austria

michael.roland (at) fh-hagenberg.at

This work is part of the project "High Speed RFID" within the EU program "Regionale Wettbewerbsfähigkeit OÖ 2007–2013 (Regio 13)" funded by the European regional development fund (ERDF) and the Province of Upper Austria (Land Oberösterreich).

NFC Research Lab Hagenberg • www.nfc-research.at
A research group of the University of Applied Sciences Upper Austria